ANNALES

DE

L'INSTITUT FOURIER

Andrea BANDINI & Ignazio LONGHI

Selmer groups for elliptic curves in $\mathbb{Z}_l^d$-extensions of function fields of characteristic p

Tome 59, n^{o} 6 (2009), p. 2301-2327.

<http://aif.cedram.org/item?id=AIF_2009__59_6_2301_0>

© Association des Annales de l'institut Fourier, 2009, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (http://aif.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://aif.cedram.org/legal/). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Ann. Inst. Fourier, Grenoble
59, 6 (2009) 2301-2327

SELMER GROUPS FOR ELLIPTIC CURVES IN $\mathbb{Z}_l^d$-EXTENSIONS OF FUNCTION FIELDS OF CHARACTERISTIC p

by Andrea BANDINI & Ignazio LONGHI

Abstract. — Let F be a function field of characteristic $p > 0$, $\mathcal{F}/F$ a $\mathbb{Z}_l^d$-extension (for some prime $l \neq p$) and E/F a non-isotrivial elliptic curve. We study the behaviour of the r-parts of the Selmer groups (r any prime) in the subextensions of $\mathcal{F}$ via appropriate versions of Mazur's Control Theorem. As a consequence we prove that the limit of the Selmer groups is a cofinitely generated (in some cases cotorsion) module over the Iwasawa algebra of $\mathcal{F}/F$.

Résumé. — Soit F un corps de fonctions de caractéristique $p > 0$, $\mathcal{F}/F$ une $\mathbb{Z}_l^d$-extension (pour un nombre premier $l \neq p$) et E/F une courbe elliptique non-isotrivale. Nous étudions le comportement des r-parties des groupes de Selmer pour les sous-extensions de $\mathcal{F}$ par des variantes du Théorème de contrôle de Mazur. Conséquemment, nous démontrons que la limite des groupes de Selmer est un module finiment co-engendré (parfois de cotorsion) sur l'algèbre d'Iwasawa de $\mathcal{F}/F$.

1. Introduction

Let F be a function field (in the whole paper function field means a field of transcendence degree 1 over its constant field) with constant field $\mathbb{F}$ an intermediate extension between $\mathbb{F}_p$ (the field with p elements) and a (fixed) algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. Let E/F be a non-isotrivial elliptic curve (*i.e.,* $j(E) \notin \mathbb{F}$) and assume that E has good or split multiplicative reduction at all primes of F (it is always possible to reduce to this situation by simply taking a finite extension of F).

Let l be a prime different from p, let $\mathcal{F}/F$ be a $\mathbb{Z}_l^d$-extension of F with Galois group Γ (the case $l = p$ has been developed in [2] for global function fields). Denote by $\Lambda := \mathbb{Z}_l[[\Gamma]]$ the associated Iwasawa algebra. Let $\mathbb{F}_p^{(l)}$ be

Keywords: Selmer groups, elliptic curves, function fields, Iwasawa theory.
Math. classification: 11G05, 11R23.

the unique $\mathbb{Z}_l$-extension of $\mathbb{F}_p$. If $\mathbb{F}_p^{(l)} \not\subset \mathbb{F}$ then there is only one $\mathbb{Z}_l$-extension of F, namely the arithmetic one, obtained by extending scalars from $\mathbb{F}$ to $\mathbb{F}_p^{(l)}\mathbb{F}$ (see Proposition 4.3); we recall that this extension is everywhere unramified. On the other hand, if, for example, $\mathbb{F}$ contains $\boldsymbol{\mu}_{l^\infty}$ (the roots of unity of l-power order) then Kummer theory produces lots of examples of disjoint $\mathbb{Z}_l$-extensions of F (see the Appendix).

In section 2 we will define the r-part (r any prime) of the Selmer group of E, $\mathrm{Sel}_E(L)_r$, for any algebraic extension L of F. Our goal is to study the structure of $\mathrm{Sel}_E(\mathcal{F})_r$ (actually of its Pontrjagin dual) as a $\mathbb{Z}_r[[\Gamma]]$-module.

Not surprisingly the most interesting case happens to be $r = l$. Let $\mathcal{S}$ be the Pontrjagin dual of $\mathrm{Sel}_E(\mathcal{F})_l$: its structure depends, among other things, on the base field $\mathbb{F}$. Namely we have different results depending on whether $\mathbb{F}_p^{(l)} \subset \mathbb{F}$ or not. In section 4, we shall prove the following

Theorem 1.1. — *Assume that $\mathbb{F}$ does not contain $\mathbb{F}_p^{(l)}$. Then $\mathcal{S}$ is a finitely generated Λ-module. Moreover if $\mathrm{Sel}_E(F)_l$ is finite then $\mathcal{S}$ is Λ-torsion.*

Theorem 1.2. — *Assume that only finitely many primes of F are ramified in $\mathcal{F}/F$ and that $\mathbb{F}$ contains $\mathbb{F}_p^{(l)}$. Then $\mathcal{S}$ is a finitely generated Λ-module.*

Moreover if:

1. *the ramified primes are of good reduction for E;*
2. *for any ramified prime v, $E[l^\infty](F_v)$ is finite (F_v is the completion of F at v);*
3. *$\mathrm{Sel}_E(F)_l$ is finite,*

then $\mathcal{S}$ is Λ-torsion.

Remark 1.3. — When F is a global function field, according to the Birch and Swinnerton-Dyer conjecture, $\mathrm{Sel}_E(F)_l$ is finite if and only if $\mathrm{rank}\, E(F) = 0$.

When $\mathcal{F}/F$ is a $\mathbb{Z}_l$-extension and $\mathcal{S}$ is Λ-torsion it is quite easy to prove that $E(\mathcal{F})$ is finitely generated (see Corollary 4.15). The behaviour of the rank of E in an infinite tower of extensions of a function field K (in any characteristic) has been addressed by many authors. Among others, Shioda [18], Fastenberg [5] and Silverman [22] have provided examples of elliptic curves with bounded rank in towers of function fields in characteristic 0 and Ulmer [25] gives instances of the same phenomenon for elliptic curves over $\overline{\mathbb{F}}_q(t^{1/r^m})$ (r a prime not dividing q). In the opposite direction examples of elliptic curves with unbounded rank have been given by Shioda [18] for the tower $\overline{\mathbb{F}}_p(t^{1/r^m})$ and Ulmer [24] for $\mathbb{F}_p(t^{1/r^m})$. In the same spirit the structure of Selmer groups has been studied by Ellenberg [4] from a slightly different (more geometric) viewpoint using formulas on Euler characteristic for Λ-modules.

Since Mazur's classical work [10], duals of Selmer groups have provided the algebraic counterpart for p-adic L-functions in Iwasawa theory of elliptic curves over number fields. In section 4.3.2 we speculate about such an application of our results when F is a global field.

The main tools for the proofs of Theorems 1.1 and 1.2 are appropriate versions of Mazur's Control Theorem (originally proved in [10]; for a different approach, closer to ours, see [6] and [7]), which we prove in section 4 as well, and Theorem 3.6, a generalization of Nakayama's Lemma which has been proved in [1]. We follow some of the basic ideas developed in [2] for the case $l = p$.

Moreover we can prove a version of the control theorem for $\mathrm{Sel}_E(\mathcal{F})_r$ for $r \neq l$ as well, but, unfortunately, $\mathrm{Sel}_E(\mathcal{F})_r$ is a module over $\mathbb{Z}_r[[\Gamma]]$, a ring which we know very little about. Nevertheless we can say something on the structure of $\mathrm{Sel}_E(\mathcal{F})_r$ and we gathered the results on that module in section 5.

The paper ends with a short Appendix which provides a classification of $\mathbb{Z}_l^d$-extensions of a field F containing $\boldsymbol{\mu}_{l^\infty}$.

Acknowledgements. — The authors would like to thank S. Petersen for comments on an earlier version and for pointing out the idea for the proof of Proposition 4.3, F. Trihan and F. Andreatta for helpful suggestions and discussions. We are grateful to the anonymous referee for comments which led to improvements in the paper.

While this paper was written, the second author was supported by a postdoctoral scholarship of Università di Milano.

2. The setting and the Selmer groups

2.1. Notations

We list some notations which will be used throughout the paper and briefly describe the setting in which the theory will be developed.

2.1.1. Fields

Let L be a field: then L^{sep} will denote a separable algebraic closure of L and we put $G_L := \mathrm{Gal}(L^{\mathrm{sep}}/L)$. Moreover $\overline{L}$ will denote an algebraic closure of L.

If L is a global field (or an algebraic extension of such), $\mathcal{M}_L$ will be its set of places. For any place $v \in \mathcal{M}_L$ we let L_v be the completion of L at v, $\mathcal{O}_v$ the ring of integers of L_v, ord_v the valuation associated to v and $\mathbb{L}_v$ the residue field.

As usual, $\boldsymbol{\mu}_n$ denotes the group of n-th roots of 1.

As stated in the introduction, we fix a function field F of characteristic $p > 0$ and an algebraic closure $\overline{F}$. Its constant field will be denoted by $\mathbb{F}$. Then F is generated over $\mathbb{F}$ by a finite number of transcendental elements $z_0, \dots, z_n$ subjected to algebraic relations. These relations are defined over some finite field $\mathbb{F}_q \subset \mathbb{F}$ for $q \gg 0$. Let $F_0 := \mathbb{F}_q(z_0, \dots, z_n)$: then F_0 is a global field, $F = \mathbb{F}F_0$ and $\mathrm{Gal}(F/F_0) \simeq \mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$.

For any place $v \in \mathcal{M}_F$ we choose $\overline{F_v}$ and an embedding $\overline{F} \hookrightarrow \overline{F_v}$, so to get a corresponding inclusion $G_{F_v} \hookrightarrow G_F$. All algebraic extensions of F (resp. of F_v) will be assumed to be contained in $\overline{F}$ (resp. in $\overline{F_v}$).

Script letters will denote infinite extensions of F; in particular $\mathcal{F}/F$ will be a $\mathbb{Z}_l^d$-extension with l a fixed prime different from p. We shall consider a sequence of finite extensions of F such that

$$F \subset F_1 \subset \cdots \subset F_n \subset \cdots \subset \bigcup F_n = \mathcal{F}.$$

In this setting we let $\Gamma := \mathrm{Gal}(\mathcal{F}/F)$ and $\Gamma_n := \mathrm{Gal}(\mathcal{F}/F_n)$ (for any $n > 0$).

For γ an element in a profinite group, $\overline{\langle\gamma\rangle}$ will denote the closed subgroup topologically generated by γ.

2.1.2. Elliptic curves

We fix a non-isotrivial elliptic curve E/F, having split multiplicative reduction at all places supporting its conductor. The reader is reminded that then at such places E is isomorphic to a Tate curve, *i.e.*, $E(F_v) \simeq F_v^*/q_{E,v}^{\mathbb{Z}}$ for some $q_{E,v}$ (the *Tate period* at v) with $\mathrm{ord}_v(q_{E,v}) = -\mathrm{ord}_v(j(E)) > 0$.

For any positive integer n let $E[n]$ be the scheme of n-torsion points. Moreover, for any prime r, let $E[r^\infty] := \varinjlim E[r^n]$.

By the theory of the Tate curve, if v is of bad reduction for E and $r \neq p$ one has an isomorphism of Galois modules

$$E[r^\infty](\overline{F_v}) \simeq \langle \boldsymbol{\mu}_{r^\infty}, \sqrt[r^\infty]{q_{E,v}} \rangle / q_{E,v}^{\mathbb{Z}}.$$

For any $v \in \mathcal{M}_F$ we choose a minimal Weierstrass equation for E. Let E_v be the reduction of E modulo v and for any point $P \in E$ let P_v be its image in E_v.

For all basic facts about elliptic curves, the reader is referred to Silverman's books [20] and [21].

We remark that by increasing q (if necessary) we can (and will) assume that E is defined over the field F_0 described in section 2.1.1.

2.1.3. Duals

For X a topological abelian group, we denote its Pontrjagin dual by $X^\vee := \mathrm{Hom}_{\mathrm{cont}}(X, \mathbb{C}^*)$. In the cases considered in this paper, X will be a (mostly discrete) topological $\mathbb{Z}_r$-module for some prime r, so that $X^\vee = \mathrm{Hom}_{\mathrm{cont}}(X, \mathbb{Q}_r/\mathbb{Z}_r)$ and it has a natural structure of $\mathbb{Z}_r$-module.

The reader is reminded that to say that an R-module X (R any ring) is cofinitely generated means that $X^\vee$ is a finitely generated R-module. Since $(X^\vee)^\vee \simeq X$, a module X is $\mathbb{Z}_r$-cofinitely generated if and only if it is the direct sum of a finite (r-primary) abelian group with $(\mathbb{Q}_r/\mathbb{Z}_r)^t$ for some $t \in \mathbb{N}$; in particular, letting X_{div} be the divisible part of X, we see that X/X_{div} is finite.

2.2. Selmer groups

We shall deal with torsion subschemes of the elliptic curve E. Since $\mathrm{char}\, F = p$, in order to deal with the p-torsion we need to consider flat cohomology of group schemes to define the Selmer groups in that case.

For the basic theory of sites and cohomology on a site see [11, Chapters II, III]. We define our Selmer groups via flat cohomology (for the relation with classical Galois cohomology see Remark 2.2 below) so, when we write a scheme X, we always mean the site X_{fl}.

Let L be an algebraic extension of F and $X_L := \mathrm{Spec}\, L$. For any positive integer m the group schemes $E[m]$ and E define sheaves on X_L (see [11, II.1.7]): for example $E[m](X_L) := E[m](L)$. Consider the exact sequence

$$E[m] \hookrightarrow E \xrightarrow{m} E$$

and take flat cohomology to get

$$E(L)/mE(L) \hookrightarrow H^1_{fl}(X_L, E[m]) \to H^1_{fl}(X_L, E).$$

In particular let m run through the powers r^n of a prime r. Taking direct limits one gets an injective map (a "Kummer homomorphism")

$$\kappa\colon E(L) \otimes \mathbb{Q}_r/\mathbb{Z}_r \hookrightarrow \varinjlim_n H^1_{fl}(X_L, E[r^n]) =: H^1_{fl}(X_L, E[r^\infty]).$$

As above one can build local Kummer maps for any place $v \in \mathcal{M}_L$

$$\kappa_v\colon E(L_v) \otimes \mathbb{Q}_r/\mathbb{Z}_r \hookrightarrow H^1_{fl}(X_{L_v}, E[r^\infty])$$

where $X_{L_v} := \mathrm{Spec}\, L_v$.

Definition 2.1. — *The* r-part of the Selmer group *of* E *over* L*, denoted by* $\mathrm{Sel}_E(L)_r$*, is defined to be*

$$\mathrm{Sel}_E(L)_r := \mathrm{Ker}\left\{ H^1_{fl}(X_L, E[r^\infty]) \to \prod_{v\in\mathcal{M}_L} H^1_{fl}(X_{L_v}, E[r^\infty])/\operatorname{Im}\kappa_v \right\}$$

where the map is the product of the natural restrictions between cohomology groups.

The reader is reminded that if L/F is finite then $\mathrm{Sel}_E(L)_r$ is a cofinitely generated $\mathbb{Z}_r$-module. Moreover the *Tate-Shafarevich group* $Ш(E/L)$ fits into the exact sequence

$$E(L)\otimes\mathbb{Q}_r/\mathbb{Z}_r \hookrightarrow \mathrm{Sel}_E(L)_r \twoheadrightarrow Ш(E/L)[r^\infty].$$

According to the function field version of the Birch and Swinnerton-Dyer conjecture, $Ш(E/L)$ is finite for any global function field L. Applying to this last sequence the exact functor $\mathrm{Hom}(\cdot,\mathbb{Q}_r/\mathbb{Z}_r)$, it follows that

$$\mathrm{rank}_{\mathbb{Z}_r}\mathrm{Sel}_E(L)_r^\vee = \mathrm{rank}_{\mathbb{Z}} E(L)$$

(recall that cohomology groups, hence the Selmer groups, are endowed with the discrete topology).

Fix a $\mathbb{Z}_l^d$-extension $\mathcal{F}/F$ with l a prime different from p. We will study the behaviour of the r-Selmer groups while L varies through the subextensions F_n of $\mathcal{F}/F$. Such groups admit natural actions of $\mathbb{Z}_r$, because of the torsion of E, and of $\Gamma = \mathrm{Gal}(\mathcal{F}/F)$. Hence they are modules over the Iwasawa algebra $\mathbb{Z}_r[[\Gamma]]$. When $r = l$ this algebra is (noncanonically) isomorphic to the ring of formal power series $\mathbb{Z}_l[[T_1,\dots,T_d]]$ (while, for $r\neq l$, $\mathbb{Z}_r[[\Gamma]]$ is more mysterious and we know virtually nothing about its structure).

In particular we will be concerned with the natural maps between $\mathbb{Z}_r[[\Gamma]]$-modules

$$\mathrm{Sel}_E(F_n)_r \to \mathrm{Sel}_E(\mathcal{F})_r^{\Gamma_n}.$$

Remark 2.2. — To define $\mathrm{Sel}_E(L)_r$ (with $r\neq p$) we can also use the sequence

$$E[r^n](\overline{F}) \hookrightarrow E(F^{\mathrm{sep}}) \xrightarrow{r^n} E(F^{\mathrm{sep}})$$

and classical Galois (= étale) cohomology since, in this case,

$$H^1_{fl}(X_L, E[r^n]) \simeq H^1_{et}(X_L, E[r^n]) \simeq H^1(G_L, E[r^n](\overline{F}))$$

(see [11, III.3.9]). To ease notations in this case we shall write $H^i(L,\cdot)$ instead of $H^i(G_L,\cdot)\simeq H^i_{fl}(X_L,\cdot)$ and write $E[n]$ for $E[n](\overline{F})$, putting $E[r^\infty] := \bigcup E[r^n]$. In this case the Kummer map

$$\kappa\colon E(L)\otimes\mathbb{Q}_r/\mathbb{Z}_r \hookrightarrow H^1(L, E[r^\infty])$$

has an explicit description as follows. Let $\alpha \in E(L)\otimes\mathbb{Q}_r/\mathbb{Z}_r$ be represented by $\alpha = P\otimes\frac{a}{r^k}$ $(a\in\mathbb{Z})$ and let $Q\in E(L^{\mathrm{sep}})$ be such that $aP = r^kQ$. Then $\kappa(\alpha)=\varphi_\alpha$, where $\varphi_\alpha(\sigma) := \sigma(Q)-Q$ for any $\sigma\in G_L$.

3. Auxiliary lemmas

We gather here the results which are needed for the proofs of the main theorems. We start by giving a more precise description of $\operatorname{Im}\kappa_v$ (following the path traced by Greenberg in [6] and [7]). In our situation the local conditions for the Selmer groups are easily seen to be often trivial (*i.e.,* $\operatorname{Im}\kappa_v = 0$ in general), a fact which is essentially due to $r\neq \operatorname{char} F$.

Proposition 3.1. — *Let L be the completion of an algebraic extension of F_v and r a prime different from p: then $E(L)\otimes\mathbb{Q}_r/\mathbb{Z}_r = 0$ (i.e., the Kummer map has trivial image).*

Proof. — This is an easy exercise: see *e.g.* [2, Proposition 3.3]. □

The following two lemmas deal with torsion points in abelian extensions of function fields of characteristic p both in the global and local case.

Lemma 3.2. — *Let $\mathcal{F}/F$ be a $\mathbb{Z}_l^d$-extension of function fields of characteristic $p>0$ and let E/F be a non-isotrivial elliptic curve. Then the group $E(\mathcal{F})_{\mathrm{tor}}$ is finite.*

Proof (sketch). — One proves a stronger statement: namely, that $E(L)_{\mathrm{tor}}$ is finite for any abelian extension L/F. Finiteness of $E[p^\infty](L)$ follows from the fact that points in $E[p^\infty]$ are inseparable over F (a proof can be found *e.g.* in [3, Proposition 3.8]). For the prime-to-p part, it is shown in [3, Theorem 4.2] that the claim is a consequence of the following facts:

1. $\mathrm{Gal}(F(E[r])/F)$ contains $SL_2(\mathbb{F}_r)$ for almost all primes r;
2. $\mathrm{Gal}(F(E[r^\infty])/F)$ contains S_n for some n (for any prime $r\neq p$) where S_n is the kernel of the natural reduction map $SL_2(\mathbb{Z}_r)\to SL_2(\mathbb{Z}/r^n\mathbb{Z})$.

Both statements follow from a theorem of Igusa [9]. For a clear statement we refer to [3], where however appears the hypothesis that F is global. So here we just show how to deduce **1** and **2** in the case F is not global.

Let F_0 be the global field described in section 2.1.1 and let $F' = F\cap F_0(E[r^\infty])$ (see the diagram below). The group $\mathrm{Gal}(F'/F_0)$ is abelian because it is a quotient of $\mathrm{Gal}(F/F_0)\simeq\mathrm{Gal}(\mathbb{F}/\mathbb{F}_q)$. Since $\mathrm{Gal}(F'/F_0)\simeq$

$\mathrm{Gal}(F_0(E[r^\infty])/F_0)/\mathrm{Gal}(F_0(E[r^\infty])/F')$, one has that $\mathrm{Gal}(F_0(E[r^\infty])/F')$ contains the commutators of $\mathrm{Gal}(F_0(E[r^\infty])/F_0)$. By Igusa's theorem $\mathrm{Gal}(F_0(E[r^\infty])/F_0) \supset S_n$ therefore

$$S_{2n+2} \subset [S_n, S_n] \subset \mathrm{Gal}(F_0(E[r^\infty])/F')$$

(for the inclusion on the left see *e.g.* [3, Lemma 4.1]). Since $FF_0(E[r^\infty]) = F(E[r^\infty])$ and the extensions F/F' and $F_0(E[r^\infty])/F'$ are disjoint, one gets $\mathrm{Gal}(F(E[r^\infty])/F) \simeq \mathrm{Gal}(F_0(E[r^\infty])/F')$ so $\mathrm{Gal}(F(E[r^\infty])/F) \supset S_{2n+2}$ as well.

$$\begin{tikzcd}
 & F(E[r^\infty]) \arrow[dl, dash] \arrow[dr, dash, "\supset[S_n,S_n]\supset S_{2n+2}"] & \\
F_0(E[r^\infty]) \arrow[dr, dash, "\supset[S_n,S_n]"] \arrow[ddr, dash, "S_n\subset"'] & & F \arrow[dl, dash] \\
 & F' = F_0(E[r^\infty]) \cap F \arrow[d, dash] & \\
 & F_0 &
\end{tikzcd}$$

This proves **2**. The same proof works for **1** as well (with r in place of r^∞), remembering that $SL_2(\mathbb{F}_r)$ is its own commutator subgroup for all primes $p \geqslant 5$. □

LEMMA 3.3. — *Let K be a field of characteristic p complete with respect to a discrete valuation v and with residue field $\mathbb{K} \subset \overline{\mathbb{F}}_p$. Let r be a prime different from p and assume that $\mathbb{K}$ does not contain $\mathbb{F}_p^{(r)}$ (the $\mathbb{Z}_r$-extension of $\mathbb{F}_p$). Let E/K be a non-isotrivial elliptic curve. Then $E[r^\infty](K)$ is finite.*

Proof. — Let t be a uniformizer: then $K = \mathbb{K}((t))$ and exists s such that E is defined over $K_0 := \mathbb{F}_s((t))$. Since K_0 is a local field it is easy to see that $E[r^\infty](K_0)$ is finite. Moreover since $\mathbb{F}_p^{(r)} \not\subset \mathbb{K}$, the Galois group $\mathrm{Gal}(K/K_0) \simeq \mathrm{Gal}(\mathbb{K}/\mathbb{F}_s)$ contains no copies of $\mathbb{Z}_r$.

If $E[r^\infty](K)$ is infinite then choose an infinite sequence of points $P_n \in E[r^n](K)$ such that $rP_{n+1} = P_n$ for any n. Let $K' = K_0(\{P_n\}_{n\in\mathbb{N}})$ and $\mathcal{P}$ the subgroup of $E[r^\infty]$ generated by the P_n's. Then K'/K_0 is an infinite extension and, since $K' \subset K$, one has

$$\mathrm{Gal}(K/K_0) \twoheadrightarrow \mathrm{Gal}(K'/K_0) \hookrightarrow \mathrm{Aut}(\mathcal{P}) \simeq \mathbb{Z}_r^* :$$

contradiction. □

Lemma 3.4. — *Let $\Gamma \simeq \mathbb{Z}_l^d$ and B a cofinitely generated discrete $\mathbb{Z}_l$-module with a continuous Γ-action. Assume that there exists a set $\gamma_1, \dots, \gamma_d$ of independent topological generators of Γ such that $B^{\overline{\langle\gamma_1\rangle}}$ is finite. Then, with $b := \max\{|B/B_{\mathrm{div}}|, |B^{\overline{\langle\gamma_1\rangle}}|\}$, one has*

$$|H^1(\Gamma, B)| \leqslant b^d \text{ and } |H^2(\Gamma, B)| \leqslant b^{\frac{d(d-1)}{2}}.$$

Proof. — If B is finite then $b = |B|$ and the proof is in [2, Lemma 4.1]. For the other case fix a set of independent topological generators of Γ as above and put $\gamma := \gamma_1$. Consider the exact sequence

$$0 = B_{\mathrm{div}}^{\overline{\langle\gamma\rangle}} \hookrightarrow B_{\mathrm{div}} \xrightarrow{\gamma-1} B_{\mathrm{div}} \twoheadrightarrow B_{\mathrm{div}}/(\gamma-1)B_{\mathrm{div}}$$

(because of the hypothesis on B). Taking duals one finds a sequence

$$(B_{\mathrm{div}}/(\gamma-1)B_{\mathrm{div}})^\vee \hookrightarrow (B_{\mathrm{div}})^\vee \twoheadrightarrow (B_{\mathrm{div}})^\vee \simeq \mathbb{Z}_l^t$$

(for some finite t) and, counting ranks,

$$\mathrm{rank}_{\mathbb{Z}_l}(B_{\mathrm{div}}/(\gamma-1)B_{\mathrm{div}})^\vee = 0.$$

Therefore $(B_{\mathrm{div}}/(\gamma-1)B_{\mathrm{div}})^\vee$ is finite and, since $\mathbb{Z}_l^t$ has no nontrivial finite subgroup, one finds

$$B_{\mathrm{div}}/(\gamma-1)B_{\mathrm{div}} = 0.$$

Hence $B_{\mathrm{div}} = (\gamma-1)B_{\mathrm{div}} \subset (\gamma-1)B \subset B$ yields

$$|B/(\gamma-1)B| \leqslant |B/B_{\mathrm{div}}|.$$

Now we use induction on d. For $d = 1$ the equality $\Gamma = \overline{\langle\gamma\rangle}$ implies $H^1(\Gamma, B) \simeq B/(\gamma-1)B$ and $H^2(\Gamma, B) = 0$ (because $\mathbb{Z}_l$ has l-cohomological dimension 1, see [14, Proposition 3.5.9]).

For $d > 1$ let $\Gamma/\overline{\langle\gamma\rangle} =: \Gamma' \simeq \mathbb{Z}_l^{d-1}$. The inflation restriction sequence

$$H^1(\Gamma', B^{\overline{\langle\gamma\rangle}}) \hookrightarrow H^1(\Gamma, B) \to H^1(\overline{\langle\gamma\rangle}, B)$$

yields

$$|H^1(\Gamma, B)| \leqslant |H^1(\Gamma', B^{\overline{\langle\gamma\rangle}})|\ |H^1(\overline{\langle\gamma\rangle}, B)| \leqslant b^{d-1}b.$$

Moreover since $H^n(\overline{\langle\gamma\rangle}, B) = 0$ for any $n \geqslant 2$, the Hochschild-Serre spectral sequence (see [14, Theorem 2.1.5 and Exercise 5, page 96]) gives an exact sequence

$$H^2(\Gamma', B^{\overline{\langle\gamma\rangle}}) \to H^2(\Gamma, B) \to H^1(\Gamma', H^1(\overline{\langle\gamma\rangle}, B)).$$

By induction and the bound on $|H^1(\overline{\langle\gamma\rangle}, B)|$ one has

$$\begin{aligned}|H^2(\Gamma, B)| &\leqslant |H^2(\Gamma', B^{\overline{\langle\gamma\rangle}})|\ |H^1(\Gamma', H^1(\overline{\langle\gamma\rangle}, B))| \\ &\leqslant b^{\frac{(d-1)(d-2)}{2}} b^{d-1} = b^{\frac{d(d-1)}{2}}.\end{aligned}$$

□

Remark 3.5. — Notice that if $d = 1$ we have proved a slightly stronger statement, namely that

$$B^\Gamma \text{ finite } \Longrightarrow |H^1(\Gamma, B)| \leqslant |B/B_{\mathrm{div}}|.$$

To conclude we mention the version of Nakayama's Lemma we are going to use in what follows: its proof (and further generalizations) can be found in [1].

Theorem 3.6. — *Let Λ be a compact topological ring with 1 and let I be an ideal such that $I^n \to 0$. Assume that X is a profinite Λ-module. If X/IX is a finitely generated Λ/I-module then X is a finitely generated Λ-module and the number of generators of X over Λ is at most the number of generators of X/IX over Λ/I. Moreover if $\Lambda = \mathbb{Z}_l[[\Gamma]]$, $I := \mathrm{Ker}\{\Lambda \to \mathbb{Z}_l\}$ is the augmentation ideal and X/IX is finite then X is Λ-torsion.*

4. Control theorems for $\mathrm{Sel}_E(\mathcal{F})_r$ $(r \neq p)$

Before going on with the main theorems we describe the extensions we are going to deal with. We recall that $\mathbb{F}_p^{(r)}$ denotes the unique $\mathbb{Z}_r$-extension of $\mathbb{F}_p$.

Lemma 4.1. — *For any prime $r \neq p$, the following statements are equivalent:*

1. $\mathbb{F}_p^{(r)} \subseteq \mathbb{F}$;
2. $\boldsymbol{\mu}_{r^\infty} \subset \mathbb{F}(\boldsymbol{\mu}_r)$;
3. $\mathbb{Z}_r \hookrightarrow \mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$.

Proof. — Obvious, just recall that

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \simeq \widehat{\mathbb{Z}} := \prod_r \mathbb{Z}_r$$

and

$$\mathbb{F}_p^{(r)} = \mathbb{F}_p(\boldsymbol{\mu}_{r^\infty})^{\mathrm{Gal}(\mathbb{F}_p(\boldsymbol{\mu}_r)/\mathbb{F}_p)}.$$

□

Lemma 4.2. — *Let v be any place of F, w a place of $\mathcal{F}$ dividing v and* $\Gamma_v := \mathrm{Gal}(\mathcal{F}_w/F_v)$. *One has that:*

1. *if* $\boldsymbol{\mu}_{l^\infty} \not\subset F_v$, *then*

$$\Gamma_v \simeq \begin{cases} \mathbb{Z}_l & \text{if } v \text{ is inert} \\ 0 & \text{otherwise} \end{cases};$$

2. *if* $\boldsymbol{\mu}_{l^\infty} \subset F_v$, *then*

$$\Gamma_v \simeq \begin{cases} \mathbb{Z}_l & \text{if } v \text{ is totally ramified} \\ 0 & \text{otherwise} \end{cases}.$$

Proof. — For any finite subextension L/F_v of $\mathcal{F}_w/F_v$ we have an exact sequence

$$I(L/F_v) \hookrightarrow \mathrm{Gal}(L/F_v) \twoheadrightarrow \mathrm{Gal}(\mathbb{L}/\mathbb{F}_v)$$

where I denotes the inertia subgroup. Since $\mathcal{F}_w/F_v$ is tamely ramified, there is an injective homomorphism $I(L/F_v) \hookrightarrow \mathbb{F}_v^*$ (see *e.g.* [17, IV, 2, Corollary 1 of Proposition 7]), hence $|I(L/F_v)| \leqslant |\boldsymbol{\mu}_{l^\infty}(F_v)|$. There are two cases.

Case 1: $\boldsymbol{\mu}_{l^\infty} \not\subset F_v$. Since $I(\mathcal{F}_w/F_v)$ is a submodule of the free $\mathbb{Z}_l$-module Γ_v, it follows from the boundedness of $|\boldsymbol{\mu}_{l^\infty}(F_v)|$ and the equality $I(\mathcal{F}_w/F_v) = \varprojlim I(L/F_v)$ that all these groups are trivial. Therefore, either $\Gamma_v \simeq \mathrm{Gal}(\mathbb{F}_v^{(l)}/\mathbb{F}_v)$ and $\mathcal{F}_w$ is the constant field extension $\mathbb{F}_v^{(l)}F_v$ or $\mathcal{F}_w = F_v$.

Case 2: $\boldsymbol{\mu}_{l^\infty} \subset F_v$. In this case $\mathbb{F}_p^{(l)} \subset \mathbb{F}_v$ and $\mathbb{F}_v$ has no l-extensions: hence either $\mathcal{F}_w = F_v$ or $\mathcal{F}_w/F_v$ is totally ramified. One can apply Kummer theory to the classification of $\mathbb{Z}_l$-extensions, as described in the Appendix. Let t be a uniformizer of the complete discrete valuation field F_v: from $F_v^* = \mathbb{F}_v^* \times t^{\mathbb{Z}} \times (1\text{-units})$ it follows that the l-adic completion of F_v^* is $t^{\mathbb{Z}_l}$, hence the only $\mathbb{Z}_l$-extension is $F_v(\sqrt[l^\infty]{t})$. □

Proposition 4.3. — *If* $\mathbb{F}_p^{(l)} \not\subset \mathbb{F}$ *then F has a unique $\mathbb{Z}_l$-extension, namely the constant field extension* $\mathbb{F}_p^{(l)}F$.

For the proof, we remind the reader that F is the function field of a smooth, projective connected curve $\mathcal{C}$ defined over $\mathbb{F}$. Remembering that $F = \mathbb{F}F_0$, one sees that $\mathcal{C}$ can be obtained by base change from a curve $\mathcal{C}_0$ defined over $\mathbb{F}_q$. Let g be the genus of $\mathcal{C}_0$ and $\mathcal{C}$.

Proof. — Fix a geometric point P of $\mathcal{C}$. By Lemma 4.2 one sees that a $\mathbb{Z}_l^d$-extension $\mathcal{F}/F$ is everywhere unramified: therefore there is a surjective morphism ϕ from the fundamental group $\pi_1(\mathcal{C}, P)$ to $\mathrm{Gal}(\mathcal{F}/F)$.

We can assume that the point P lies in $\mathcal{C}(\mathbb{F})$ (otherwise just take a finite extension of F whose constant field obviously still does not contain $\mathbb{F}_p^{(l)}$). Then we have a split exact sequence of fundamental groups

$$\begin{tikzcd} \pi_1(\mathcal{C}\times\overline{\mathbb{F}}_p, P) \arrow[r, hook] & \pi_1(\mathcal{C}, P) \arrow[r, two heads] & G_{\mathbb{F}} \arrow[l, bend right] \end{tikzcd},$$

that is, $\pi_1(\mathcal{C}, P) \simeq \pi_1(\mathcal{C}\times\overline{\mathbb{F}}_p, P) \rtimes G_{\mathbb{F}}$. Since $\mathrm{Gal}(\mathcal{F}/F)$ is abelian, the morphism ϕ factors through $\pi_1(\mathcal{C}\times\overline{\mathbb{F}}_p, P)^{ab} \rtimes G_{\mathbb{F}}$ (notice that this semidirect product is a quotient of $\pi_1(\mathcal{C}, P)$, since the $G_{\mathbb{F}}$ action on $\pi_1(\mathcal{C}\times\overline{\mathbb{F}}_p, P)$ preserves the commutator subgroup). It is well-known (see *e.g.* [12, Proposition 9.1] together with [8, XI, Théorème 2.1]) that one can identify the group $\pi_1(\mathcal{C}\times\overline{\mathbb{F}}_p, P)^{ab}$ with the (full) Tate module of $\mathrm{Jac}(\mathcal{C})$.

Since $\mathrm{Gal}(\mathcal{F}/F)$ is a pro-l group (and the [pro]-primary-decomposition of a [profinite] abelian group is preserved by automorphisms) the morphism ϕ factors further through $T_l(\mathrm{Jac}(\mathcal{C}))\rtimes G_{\mathbb{F}}$. The following lemma shows that the maximal abelian quotient of $T_l(\mathrm{Jac}(\mathcal{C}))\rtimes G_{\mathbb{F}}$ has the form $A\times G_{\mathbb{F}}$, where A is a finite group: the proposition is an immediate consequence. $\square$

Lemma 4.4. — *If $\mathbb{F}_p^{(l)}\not\subset\mathbb{F}$ then the commutator subgroup of $T_l(\mathrm{Jac}(\mathcal{C}))\rtimes G_{\mathbb{F}}$ has finite index in $T_l(\mathrm{Jac}(\mathcal{C}))$.*

Proof. — Since $G_{\mathbb{F}}$ is abelian the commutators are contained in $T_l(\mathrm{Jac}(\mathcal{C}))$. To ease notation, shorten $T_l(\mathrm{Jac}(\mathcal{C}))$ to T. We write the group law in $T\rtimes G_{\mathbb{F}}$ as

$$(a,g)(b,h) = (a+gb, gh)$$

and let $\rho\colon G_{\mathbb{F}} \to \mathrm{Aut}_{\mathbb{Z}_l}(T)$ be the homomorphism corresponding to the action of $G_{\mathbb{F}}$ on T. Then

$$\begin{aligned}(a,e)(0,h)(a,e)^{-1}(0,h)^{-1} &= (a,h)(-a,e)(0,h^{-1})\\ &= (a-ha,h)(0,h^{-1}) = (a-ha,e)\end{aligned}$$

shows that to prove our claim it is enough to find $h\in G_{\mathbb{F}}$ such that $(1-\rho(h))T$ has finite index in T. Observe that since $T\simeq\mathbb{Z}_l^{2g}$ the operator $1-\rho(h)$ belongs to $\mathrm{End}_{\mathbb{Z}_l}(T)\simeq M_{2g}(\mathbb{Z}_l)$; an easy reasoning shows that

$$[T:(1-\rho(h))T] = |\det(1-\rho(h))|_l^{-1}$$

(where $|\cdot|_l$ is normalized so that $|l|_l := l^{-1}$). Hence we just need $\det(1-\rho(h))\neq 0$.

Let $G_{\mathbb{F}_q}^{(l)}$ and $G_{\mathbb{F}}^{(l)}$ be respectively the maximal pro-l subgroup of $G_{\mathbb{F}_q}$ and $G_{\mathbb{F}}$: the hypothesis $\mathbb{F}_p^{(l)}\not\subset\mathbb{F}$ implies $[G_{\mathbb{F}_q}^{(l)} : G_{\mathbb{F}}^{(l)}] < \infty$. Since all prime-to-$l$ subgroups of $\mathrm{Aut}_{\mathbb{Z}_l}(T)\simeq GL_{2g}(\mathbb{Z}_l)$ are finite so is the index $[\rho(G_{\mathbb{F}_q}) :$

$\rho(G^{(l)}_{\mathbb{F}_q})]$. Hence there exists $h \in G^{(l)}_{\mathbb{F}}$ such that $\rho(h) = \rho(\mathrm{Frob}^n_q)$ for some n (where Frob_q is the "canonical" generator of $G_{\mathbb{F}_q}$).

The proof is concluded remarking the well-known fact that

$$\det(1 - \rho(\mathrm{Frob}^n_q)) = |\,\mathrm{Jac}(\mathcal{C}_0)(\mathbb{F}_{q^n})|$$

and the right hand-side is not 0. □

We are now ready to prove two versions of the control theorem appropriate for our setting.

4.1. The case $r = l$ with $\mathbb{F}^{(l)}_p \not\subset \mathbb{F}$

Theorem 4.5. — *Assume $\mathbb{F}^{(l)}_p \not\subset \mathbb{F}$. Then the natural maps*

$$\mathrm{Sel}_E(F_n)_l \to \mathrm{Sel}_E(\mathcal{F})^{\Gamma_n}_l$$

have finite kernels and cokernels both of bounded order.

Proof. — To ease notations, for any field L let $\mathcal{G}(L)$ be the image of $H^1(L, E[l^\infty])$ in the product

$$\prod_{w\in\mathcal{M}_L} H^1(L_w, E[l^\infty])/\operatorname{Im}\kappa_w = \prod_{w\in\mathcal{M}_L} H^1(L_w, E[l^\infty])$$

(by Proposition 3.1). We have a commutative diagram with exact rows

$$\begin{array}{ccccc}
\mathrm{Sel}_E(F_n)_l & \hookrightarrow & H^1(F_n, E[l^\infty]) & \twoheadrightarrow & \mathcal{G}(F_n) \\
\downarrow{\scriptstyle a_n} & & \downarrow{\scriptstyle b_n} & & \downarrow{\scriptstyle c_n} \\
\mathrm{Sel}_E(\mathcal{F})^{\Gamma_n}_l & \hookrightarrow & H^1(\mathcal{F}, E[l^\infty])^{\Gamma_n} & \longrightarrow & \mathcal{G}(\mathcal{F})
\end{array}$$

and we are interested in $\operatorname{Ker} a_n$ and $\operatorname{Coker} a_n$.
By the Hochschild-Serre spectral sequence one gets

$$\operatorname{Ker} b_n \simeq H^1(\Gamma_n, E[l^\infty](\mathcal{F}))$$

and

$$\operatorname{Coker} b_n \subseteq H^2(\Gamma_n, E[l^\infty](\mathcal{F})).$$

By Lemma 3.2 the group $E[l^\infty](\mathcal{F})$ is finite and by Proposition 4.3 $\Gamma_n \simeq \mathbb{Z}_l$. So Lemma 3.4 immediately gives

$$|\operatorname{Ker} b_n| \leqslant |E[l^\infty](\mathcal{F})| \quad \text{and} \quad \operatorname{Coker} b_n = 0.$$

By the snake lemma, this is enough to show that $\operatorname{Ker} a_n$ is finite and bounded independently of n.

For $\operatorname{Coker} a_n$ we need some control on $\operatorname{Ker} c_n$ as well. Obviously $\operatorname{Ker} c_n$ embeds in the kernel of the natural map

$$d_n : \prod_{v_n \in \mathcal{M}_{F_n}} H^1(F_{v_n}, E[l^\infty]) \longrightarrow \prod_{w \in \mathcal{M}_{\mathcal{F}}} H^1(\mathcal{F}_w, E[l^\infty]).$$

For any $w|v_n$ we have a map

$$d_w : H^1(F_{v_n}, E[l^\infty]) \longrightarrow H^1(\mathcal{F}_w, E[l^\infty])$$

and $w_1, w_2|v_n$ imply $\operatorname{Ker} d_{w_1} = \operatorname{Ker} d_{w_2}$. Letting d_{v_n} be the product of the d_w's for all the w's dividing v_n, we have $\operatorname{Ker} d_{v_n} = \bigcap_{w_i|v_n} \operatorname{Ker} d_{w_i} = \operatorname{Ker} d_w$ for any $w|v_n$ and

$$\operatorname{Ker} c_n \subseteq \operatorname{Ker} d_n = \prod_{v_n \in \mathcal{M}_{F_n}} \operatorname{Ker} d_{v_n}.$$

By the inflation restriction sequence $\operatorname{Ker} d_w = H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w))$ (where $\Gamma_{v_n} := \operatorname{Gal}(\mathcal{F}_w/F_{v_n})$ is independent of w since Γ is abelian).
As seen in Lemma 4.2 one finds $\Gamma_{v_n} = 0$ or $\mathbb{Z}_l$ and the latter is the only nontrivial case. Moreover $\mathcal{F}_w/F_v$ is unramified (by Lemma 4.3): therefore $\mathcal{F}_w \subset F_{v_n}^{\mathrm{unr}}$, the maximal unramified extension of F_{v_n}.

4.1.1. Places of good reduction

Assume v_n is of good reduction. By the criterion of Néron-Ogg-Shafarevich the field $F_{v_n}(E[l^\infty])$ is contained in $F_{v_n}^{\mathrm{unr}}$. The pro-l-part of $\operatorname{Gal}(F_{v_n}^{\mathrm{unr}}/F_{v_n}) \simeq \operatorname{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_{v_n})$ is isomorphic to $\mathbb{Z}_l$ because $\mathbb{F}_p^{(l)} \not\subset \mathbb{F}$ yields $\mathbb{F}_p^{(l)} \not\subset \mathbb{F}_{v_n}$ (which is a finite extension of $\mathbb{F}$). Let φ_l be a topological generator of the $\mathbb{Z}_l$-part of the Galois group $\operatorname{Gal}(F_{v_n}^{\mathrm{unr}}/F_{v_n})$. Since $H := \operatorname{Gal}(F_{v_n}^{\mathrm{unr}}/F_{v_n})/\overline{\langle\varphi_l\rangle}$ has no l-primary part and $E[l^\infty]$ is l-primary, the cohomology groups $H^i(H, E[l^\infty]^{\overline{\langle\varphi_l\rangle}})$ are trivial for $i \geqslant 1$. The Hochschild-Serre spectral sequence provides an isomorphism

$$H^1(\operatorname{Gal}(F_{v_n}^{\mathrm{unr}}/F_{v_n}), E[l^\infty]) \simeq H^1(\overline{\langle\varphi_l\rangle}, E[l^\infty])^H.$$

Note that the constant field of $F_{v_n,l} := (F_{v_n}^{\mathrm{unr}})^{\overline{\langle\varphi_l\rangle}}$ does not contain $\mathbb{F}_p^{(l)}$ because there is no $\mathbb{Z}_l$-extension between F_{v_n} and $F_{v_n,l}$. Therefore by Lemma 3.3, $E[l^\infty]^{\overline{\langle\varphi_l\rangle}} = E[l^\infty](F_{v_n,l})$ is finite. By Remark 3.5 and the fact that $E[l^\infty]$ is divisible one has $H^1(\overline{\langle\varphi_l\rangle}, E[l^\infty]) = 0$, so $H^1(\operatorname{Gal}(F_{v_n}^{\mathrm{unr}}/F_{v_n}), E[l^\infty])$ is trivial too. Since $\mathcal{F}_w \subset F_{v_n}^{\mathrm{unr}}$, the inflation map

$$H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w)) \hookrightarrow H^1(\operatorname{Gal}(F_{v_n}^{\mathrm{unr}}/F_{v_n}), E[l^\infty])$$

shows that

$$\operatorname{Ker} d_w = H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w)) = 0$$

as well.

4.1.2. Places of bad reduction

Let $\mathcal{R}_{n,i}$ be the (finite) set of primes of F_n which are of bad reduction for E and inert in $\mathcal{F}/F_n$. We recall that $\Gamma_{v_n} \simeq \mathbb{Z}_l$ only if v_n is inert (otherwise $\Gamma_{v_n} = 0$); moreover $E[l^\infty](\mathcal{F}_w)^{\Gamma_{v_n}} = E[l^\infty](F_{v_n})$ is finite by Lemma 3.3. For a prime in $\mathcal{R}_{n,i}$, using Remark 3.5 one immediately finds

$$|\operatorname{Ker} d_w| = |H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w))| \leqslant |E[l^\infty](\mathcal{F}_w)/E[l^\infty](\mathcal{F}_w)_{\mathrm{div}}|.$$

Note that such bound actually depends on v_n and not on w so, to ease notations, we choose one prime $w|v_n$ and we define

$$\varepsilon(v_n) := |E[l^\infty](\mathcal{F}_w)/E[l^\infty](\mathcal{F}_w)_{\mathrm{div}}|.$$

Therefore

$$|\operatorname{Ker} c_n| \leqslant |\operatorname{Ker} d_n| \leqslant \prod_{v_n \in \mathcal{R}_{n,i}} \varepsilon(v_n)$$

is finite and bounded as well. □

Remark 4.6. — Recall that we are assuming that E is a Tate curve at any (inert) place v_n of bad reduction, so

$$E[l^\infty](\mathcal{F}_w)_{\mathrm{div}} = \begin{cases} 0 & \text{if } \boldsymbol{\mu}_l \not\subset \mathbb{F}_v \\ \boldsymbol{\mu}_{l^\infty} & \text{if } \boldsymbol{\mu}_l \subset \mathbb{F}_v \end{cases}.$$

Besides the Tate period $q_{E,v}$ has an l^nth root in $\mathcal{F}_w$ if and only if the l-adic valuation of $\operatorname{ord}_v(q_{E,v})$ is at least n. Hence $E[l^\infty](\mathcal{F}_w)/E[l^\infty](\mathcal{F}_w)_{\mathrm{div}}$ is a cyclic group of order

$$\varepsilon(v) \leqslant \frac{1}{|\operatorname{ord}_v(q_{E,v})|_l}$$

(where $|\cdot|_l$ is the normalized l-adic absolute value). Moreover (as in Lemma 3.4) one has a surjection

$$\begin{aligned} E[l^\infty](\mathcal{F}_w)/E[l^\infty](\mathcal{F}_w)_{\mathrm{div}} \twoheadrightarrow E[l^\infty](\mathcal{F}_w)/(\gamma_{v_n}-1)E[l^\infty](\mathcal{F}_w) \\ \simeq H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w)) \end{aligned}$$

(where γ_{v_n} is a topological generator of Γ_{v_n}) which shows that $\operatorname{Ker} d_w$ is generated by one element.

Remark 4.7. — The uniform bounds provided by the theorem basically depend on the number of torsion points and the places of bad reduction. Explicitly, letting $\mathcal{R}_i$ be the set of (inert) primes of F of bad reduction for E, we found

$$|\operatorname{Ker} a_n| \leqslant |E[l^\infty](\mathcal{F})| \quad \text{and} \quad |\operatorname{Coker} a_n| \leqslant \prod_{v\in\mathcal{R}_i} \varepsilon(v).$$

Also, observe that $|E[l^\infty](\mathcal{F})|$ is bounded by the number of torsion points in the maximal abelian extension: so one could find bounds depending only on F and E.

4.2. The case $r = l$ with $\mathbb{F}_p^{(l)} \subset \mathbb{F}$

Notice that in this case, thanks to Lemmas 4.1 and 4.2, only those places v such that $\boldsymbol{\mu}_l \subset \mathbb{F}_v$ can ramify in $\mathcal{F}/F$; all the rest are totally split (since $\mathbb{F}_p^{(l)} \subset \mathbb{F}$ there is no possibility for a $\mathbb{Z}_l$-extension of the constant field corresponding to an inert $\mathbb{Z}_l$-extension of F_v).

Theorem 4.8. — *Assume that $\mathbb{F}_p^{(l)} \subset \mathbb{F}$ and that only a finite number of places of F ramify in $\mathcal{F}$. Then the natural maps*

$$\operatorname{Sel}_E(F_n)_l \to \operatorname{Sel}_E(\mathcal{F})_l^{\Gamma_n}$$

have finite and bounded kernels and cofinitely generated cokernels (of bounded corank over $\mathbb{Z}_l$ when $d = 1$).

Proof. — Exactly as in Theorem 4.5, we have a commutative diagram with exact rows

$$\begin{tikzcd}
\operatorname{Sel}_E(F_n)_l \arrow[r, hook] \arrow[d, "a_n"] & H^1(F_n, E[l^\infty]) \arrow[r, two heads] \arrow[d, "b_n"] & \mathcal{G}(F_n) \arrow[d, "c_n"] \\
\operatorname{Sel}_E(\mathcal{F})_l^{\Gamma_n} \arrow[r, hook] & H^1(\mathcal{F}, E[l^\infty])^{\Gamma_n} \arrow[r] & \mathcal{G}(\mathcal{F})
\end{tikzcd}$$

with

$$\operatorname{Ker} b_n \simeq H^1(\Gamma_n, E[l^\infty](\mathcal{F})) \quad \text{and} \quad \operatorname{Coker} b_n \subseteq H^2(\Gamma_n, E[l^\infty](\mathcal{F})).$$

Again by Lemma 3.2 the group $E[l^\infty](\mathcal{F})$ is finite. Hence Lemma 3.4 yields

$$|\operatorname{Ker} a_n| \leqslant |\operatorname{Ker} b_n| \leqslant |E[l^\infty](\mathcal{F})|^d$$

and

$$|\operatorname{Coker} b_n| \leqslant |E[l^\infty](\mathcal{F})|^{\frac{d(d-1)}{2}}.$$

As before, for $\operatorname{Coker} a_n$ we need some control on $\operatorname{Ker} c_n$ and one gets it by looking at the $\operatorname{Ker} d_w = H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w))$ for any $w|v_n$.

4.2.1. Places of good reduction

Assume $v_n|v$ of good reduction. By Lemma 4.2 we get $\Gamma_{v_n} \simeq \mathbb{Z}_l$ only if v_n is ramified (otherwise it is 0 and $\operatorname{Ker} d_w$ is trivial). Note that by the criterion of Néron-Ogg-Shafarevich

$$E[l^\infty](\mathcal{F}_w) = E[l^\infty](F_v).$$

Hence for a ramified place v_n one has (with $\Gamma_{v_n} = \overline{\langle \gamma_{v_n} \rangle}$)

$$H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w)) = E[l^\infty](F_v)/(\gamma_{v_n} - 1)E[l^\infty](F_v) = E[l^\infty](F_v)$$

which obviously has $\mathbb{Z}_l$-corank $\leqslant 2$ (notice that it can be equal to 2: for example when $\mathbb{F} = \overline{\mathbb{F}}_p$).

4.2.2. Places of bad reduction

Let v_n be one of the (finitely many) primes of bad reduction for E, lying above v. Since Γ_{v_n} is $\mathbb{Z}_l$ or 0 it is easy to see that for these ramified places

$$\operatorname{corank}_{\mathbb{Z}_l} H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w)) \leqslant 2$$

but we can be a bit more precise.

Assume v_n is ramified (otherwise $\operatorname{Ker} d_w = 0$): by the theory of the Tate curve $E[l^\infty] \simeq \langle \boldsymbol{\mu}_{l^\infty}, \sqrt[l^\infty]{q_{E,v}} \rangle / q_{E,v}^{\mathbb{Z}}$ where $q_{E,v} \in F_v$ is the Tate period (note that since $\boldsymbol{\mu}_{l^\infty} \subset \mathbb{F}_v$ the set $E[l^\infty](\mathcal{F}_w)^{\Gamma_{v_n}} = E[l^\infty](F_{v_n})$ is infinite and we cannot immediately apply Lemma 3.4). Besides $E[l^\infty](\mathcal{F}_w) = E[l^\infty]$. Therefore

$$H^1(\Gamma_{v_n}, E[l^\infty](\mathcal{F}_w)) \simeq H^1(\Gamma_{v_n}, \boldsymbol{\mu}_{l^\infty}) \times H^1(\Gamma_{v_n}, \sqrt[l^\infty]{q_{E,v}}) \simeq \boldsymbol{\mu}_{l^\infty}$$

because Γ_{v_n} acts trivially on $\boldsymbol{\mu}_{l^\infty}$ and $\sqrt[l^\infty]{q_{E,v}}$ is divisible and such that $(\sqrt[l^\infty]{q_{E,v}})^{\Gamma_{v_n}}$ is finite (use Remark 3.5).

Let's divide the set of places ramified in $\mathcal{F}/F_n$ into $\mathcal{R}_{n,g}$ (consisting of primes where E has good reduction) and $\mathcal{R}_{n,b}$ (primes of bad reduction for E). Then all the above computations lead to the bound

$$\operatorname{corank}_{\mathbb{Z}_l} \operatorname{Coker} a_n \leqslant 2|\mathcal{R}_{n,g}| + |\mathcal{R}_{n,b}|.$$

Note that, if $d > 1$, the number of ramified places is unbounded so the coranks are unbounded as well, while for $d = 1$ any ramified place of F can split only a finite number of times in $\mathcal{F}$. □

Corollary 4.9. — *In the setting of Theorem 4.8 assume that:*

1. *the ramified places are of good reduction for E;*

2. *$E[l^\infty](F_v)$ is finite for any ramified place v.*

Then the natural maps $\mathrm{Sel}_E(F_n)_l \to \mathrm{Sel}_E(\mathcal{F})_l^{\Gamma_n}$ have finite (and bounded) kernels and finite cokernels (of bounded order if $d=1$).

Proof. — Just observe that the hypotheses yield

$$\mathrm{Ker}\, d_w = \begin{cases} 0 & \text{if } v_n \text{ is unramified} \\ E[l^\infty](F_v) & \text{otherwise} \end{cases}.$$

So one has $|\,\mathrm{Coker}\, a_n| \leqslant |E[l^\infty](\mathcal{F})|^{\frac{d(d-1)}{2}} \prod_{v_n \in \mathcal{R}_{n,g}} |E[l^\infty](F_v)|$. □

Remark 4.10.

1. The assumption that only finitely many places ramify in $\mathcal{F}/F$ is strictly necessary: see Example A.2 in the appendix.

2. Hypothesis 2 in Corollary 4.9 is often satisfied. In case of good reduction, by the criterion of Néron-Ogg-Shafarevich, we have $E[l^\infty](F_{v_n}) \simeq E_{v_n}[l^\infty](\mathbb{F}_{v_n}) = E_{v_n}[l^\infty]^G$, where $G := \mathrm{Gal}(\mathbb{F}_{v_n}(E_{v_n}[l^\infty])/\mathbb{F}_{v_n})$. Let $\mathbb{F}_q$ be the field of definition of E_{v_n} and put $G_0 := \mathrm{Gal}(\mathbb{F}_{v_n}(E_{v_n}[l^\infty])/\mathbb{F}_q)$: as a quotient of $G_{\mathbb{F}_q}$, G_0 is topologically generated by the Frobenius Frob_q. We consider the embedding $G_0 \hookrightarrow \mathrm{Aut}(E_{v_n}[l^\infty]) \simeq GL_2(\mathbb{Z}_l)$: it's easy to see that $g \in G_0$ fixes a finite number of points iff it has not 1 as an eigenvalue. Assume that $\mathrm{Gal}(\mathbb{F}_{v_n}/\mathbb{F}_q) \simeq \mathbb{Z}_l$, so that if G_0 has a prime-to-l part, it must be G: in particular $G \neq \{1\}$ if the order of Frob_q in $\mathrm{Aut}(E_{v_n}[l])$ does not divide l. Suppose besides that $\mathrm{End}(E_{v_n})$ is an order $\mathcal{O}$ in a quadratic imaginary field K: then Frob_q lies in $\mathrm{End}(E_{v_n}) - \mathbb{Z}$ and it has eigenvalues $\{x, x^\tau\}$, τ a generator of $\mathrm{Gal}(K/\mathbb{Q})$.[(1)] It follows that any $g \in G_0$ has eigenvalues $\{y, y^\tau\}$ for some $y \in \overline{\langle x \rangle} \subset (\mathcal{O} \otimes \mathbb{Z}_l)^*$: in particular, if l is not split in K, $y = 1$ implies that g is the identity.

Let B be a cofinitely generated discrete $\mathbb{Z}_l$-module with a continuous Γ action and denote $h_i(B)$ the number of generators of $H^i(\Gamma, B)$ $(i = 1, 2)$. The same induction argument as in Lemma 3.4 shows that if b is the number of generators of B then

$$h_1(B) \leqslant db \quad \text{and} \quad h_2(B) \leqslant \frac{d(d-1)}{2} b.$$

One immediately finds the following corollaries (with identical proofs, so we only provide the first one).

Corollary 4.11. — *In the setting (and with the notations) of Theorem 4.5 (and the subsequent remarks) $\mathrm{Sel}_E(\mathcal{F})_l^\vee$ is a finitely generated*

(1) We are just asking that E_{v_n} is not supersingular: see [20, V.3].

Λ-module and

$$\mathrm{rank}_\Lambda \mathrm{Sel}_E(\mathcal{F})_l^\vee \leqslant \mathrm{corank}_{\mathbb{Z}_l} \mathrm{Sel}_E(F)_l + |\mathcal{R}_i|.$$

Moreover if $\mathrm{Sel}_E(F)_l$ is finite then $\mathrm{Sel}_E(\mathcal{F})_l^\vee$ is Λ-torsion.

This answers the analog of Question 1 and (some cases of) 2 in [23].

COROLLARY 4.12. — *In the setting (and with the notations) of Theorem 4.8 $\mathrm{Sel}_E(\mathcal{F})_l^\vee$ is a finitely generated Λ-module. Moreover*

$$\mathrm{rank}_\Lambda \mathrm{Sel}_E(\mathcal{F})_l^\vee \leqslant \mathrm{corank}_{\mathbb{Z}_l} \mathrm{Sel}_E(F)_l + 2|\mathcal{R}_g| + |\mathcal{R}_b| + h_2(E[l^\infty](\mathcal{F})),$$

where $\mathcal{R}_g$ (resp. $\mathcal{R}_b$) is the set of ramified places of F of good (resp. bad) reduction for E and, obviously, $h_2(E[l^\infty](\mathcal{F})) \leqslant d(d-1)$.

COROLLARY 4.13. — *In the setting of Corollary 4.9, if $\mathrm{Sel}_E(F)_l$ is finite then $\mathrm{Sel}_E(\mathcal{F})_l^\vee$ is a finitely generated torsion Λ-module.*

Proof. — Let $\mathcal{S}$ be the Pontrjagin dual of $\mathrm{Sel}_E(\mathcal{F})_l$ and let I be the augmentation ideal of Λ. The quotient $\mathcal{S}/I\mathcal{S}$ is dual to $\mathrm{Sel}_E(\mathcal{F})_l^\Gamma$ which is cofinitely generated (resp. finite) by Theorem 4.5 (resp. and the hypothesis on $\mathrm{Sel}_E(F)_l$). Therefore Theorem 3.6 yields the corollary. For the bound on the rank just use the exact sequences

$$\mathrm{Sel}_E(F)_l \to \mathrm{Sel}_E(\mathcal{F})_l^\Gamma \twoheadrightarrow \mathrm{Coker}\, a_0,$$

$$\mathrm{Ker}\, c_0 \to \mathrm{Coker}\, a_0 \to \mathrm{Coker}\, b_0 = 0$$

and recall Remarks 4.6 and 4.7. □

Remark 4.14. — For a computation of $\mathrm{rank}_\Lambda \mathcal{S}$ in the case $\mathbb{F} = \overline{\mathbb{F}}_p$ see [4, Propositions 2.5 and 3.4].

4.3. Applications

As well known, in case $d = 1$ the structure of the dual of Selmer groups can be used to control the growth of Mordell-Weil ranks in the tower of extensions between F and $\mathcal{F}$ and to formulate an “Iwasawa Main Conjecture”.

4.3.1. Mordell-Weil ranks

In [19, Theorem 1.1] Shioda proves that the group $E(F)$ is finitely generated for any function field F with algebraically closed constant field (of course this covers the case of the $\mathbb{Z}_l$-extension $\mathbb{F}_p^{(l)}F$ as well). Our Corollary 4.13 provides a new family of extensions for which $E(\mathcal{F})$ is finitely generated.

Corollary 4.15. — *In the setting of Corollary 4.9 assume that $\mathcal{F}/F$ is a $\mathbb{Z}_l$-extension and that $\mathrm{Sel}_E(F)_l$ is finite. Then $E(\mathcal{F})$ is finitely generated.*

Proof. — (More details can be found in [7, Theorem 1.3 and Corollary 4.9].) Let $\mathcal{S}$ be the dual of $\mathrm{Sel}_E(\mathcal{F})_l$: by Corollary 4.13, $\mathcal{S}$ is a finitely generated torsion Λ-module. By the well-known structure theorem for such modules there is a pseudo-isomorphism

$$\mathcal{S} \sim \bigoplus_{i=1}^{s} \mathbb{Z}_l[[T]]/(f_i^{e_i}).$$

Let $\lambda = \deg \prod f_i^{e_i}$: then $\mathrm{rank}_{\mathbb{Z}_l} \mathcal{S} = \lambda$ and, taking duals, one gets

$$(\mathrm{Sel}_E(\mathcal{F})_l)_{\mathrm{div}} \simeq (\mathbb{Q}_l/\mathbb{Z}_l)^{\lambda}.$$

By Corollary 4.9, for any n, one has

$$(\mathrm{Sel}_E(F_n)_l)_{\mathrm{div}} \simeq (\mathbb{Q}_l/\mathbb{Z}_l)^{t_n} \quad \text{with } t_n \leqslant \lambda.$$

Hence

$$(\mathbb{Q}_l/\mathbb{Z}_l)^{\mathrm{rank}\, E(F_n)} \simeq E(F_n) \otimes \mathbb{Q}_l/\mathbb{Z}_l \hookrightarrow (\mathrm{Sel}_E(F_n)_l)_{\mathrm{div}}$$

yields $\mathrm{rank}\, E(F_n) \leqslant t_n \leqslant \lambda$ for any n, *i.e.*, such ranks are bounded.

Choose m such that $\mathrm{rank}\, E(F_m)$ is maximal and let $t = |E(\mathcal{F})_{\mathrm{tor}}|$. Using the fact that $E(\mathcal{F})/E(F_m)$ is a torsion group one proves that $tP \in E(F_m)$ for all $P \in E(\mathcal{F})$ and multiplication by t gives a homomorphism $\varphi_t \colon E(\mathcal{F}) \to E(F_m)$ whose image is finitely generated and whose kernel is the finite group $E(\mathcal{F})_{\mathrm{tor}}$. Hence $E(\mathcal{F})$ is indeed finitely generated. □

4.3.2. Iwasawa Main Conjecture

When F is a global field (and, necessarily, $d = 1$ and $\mathcal{F} = \mathbb{F}_p^{(l)}F$), our control theorem may be used, as classically, as a first step towards the algebraic side for a Main Conjecture. As for the analytic side, the best candidate we know of has been provided by Pál. In [16], he constructs an element $\mathcal{L}_\infty(E)$ in the Iwasawa algebra $\mathbb{Z}[[G_\infty]] \otimes \mathbb{Q}$ (where G_∞ is the Galois group of the maximal abelian extension of F unramified outside a fixed place where E has split multiplicative reduction). He is then able to prove an interpolation formula connecting $\mathcal{L}_\infty(E)$ to a special value of the classical Hasse-Weil L-function of E ([16, Theorem 1.6]). Now, since Γ is a quotient of G_∞, there is a natural map $\pi\colon \mathbb{Z}[[G_\infty]]\otimes\mathbb{Q}\to\mathbb{Z}_l[[\Gamma]]\otimes\mathbb{Q}$. The element $\mathcal{L}_\Gamma(E):=\pi(\mathcal{L}_\infty(E))$ would then be a natural candidate for a generator of the characteristic ideal of $\mathrm{Sel}_E(\mathcal{F})_l^\vee$.

Support for such a conjecture comes from recent work of Trihan [23]. By means of techniques of syntomic cohomology, he is able to prove an Iwasawa Main Conjecture for a semistable abelian variety A/F and the $\mathbb{Z}_p$-extension $F_\infty^{(p)}:=\mathbb{F}_p^{(p)}F$ [23, Theorem 1.4]. It is not known yet what is the relation (if any) between Pal's $\mathcal{L}_\infty(E)$ and Trihan's $\mathcal{L}_{A/F_\infty^{(p)}}$ (but see [23, Remark 3.2]).

We also remark that Ochiai and Trihan [15] are able to prove that their Selmer dual is always torsion (a necessary condition to have a non-zero characteristic ideal). So one expects the analog to be true for our $\mathrm{Sel}_E(\mathcal{F})_l^\vee$ as well.

4.4. The case $r\neq l,p$

The r-part of Selmer groups behaves well in a $\mathbb{Z}_l^d$-extension: indeed it is easy to see that

THEOREM 4.16. — *The natural maps* $\mathrm{Sel}_E(F_n)_r\to\mathrm{Sel}_E(\mathcal{F})_r^{\Gamma_n}$ *are isomorphisms.*

Proof. — We use the same diagram of Theorem 4.5, only changing l-torsion with r-torsion points (since $r\neq p$ we can still use Galois cohomology). The proof goes on in the same way noting that

$$\operatorname{Ker} b_n = H^1(\Gamma_n, E[r^\infty](\mathcal{F}))=0,$$

$$\operatorname{Coker} b_n \subseteq H^2(\Gamma_n, E[r^\infty](\mathcal{F}))=0,$$

$$\operatorname{Ker} d_w = H^1(\Gamma_{v_n}, E[r^\infty](\mathcal{F}_w))=0$$

because $E[r^\infty](\mathcal{F})$ and $E[r^\infty](\mathcal{F}_w)$ are r-primary while Γ_n and Γ_{v_n} are pro-l-groups. $\square$

The consequences of this theorem on the structure of $\mathrm{Sel}_E(\mathcal{F})_r$ as a $\mathbb{Z}_r[[\Gamma]]$-module will be given in the next section together with the results on $\mathrm{Sel}_E(\mathcal{F})_p$ (see Corollary 5.3).

5. Control theorem for $\mathrm{Sel}_E(\mathcal{F})_p$

In this section we shall work with the p-torsion; so we need flat cohomology, as explained in section 2.2, and we shall follow the notations given there.

As before, it is convenient to write $\mathcal{F} = \bigcup F_n$ with F_n/F finite and $F_n \subset F_{n+1}$.

Theorem 5.1. — *The natural maps* $\mathrm{Sel}_E(F_n)_p \longrightarrow \mathrm{Sel}_E(\mathcal{F})_p^{\Gamma_n}$ *are isomorphisms.*

Proof. — We start by fixing the notations which will be used throughout the proof.

Let $X_n := \mathrm{Spec}\, F_n$, $\mathcal{X} := \mathrm{Spec}\, \mathcal{F}$, $X_{v_n} := \mathrm{Spec}\, F_{v_n}$ and $\mathcal{X}_w := \mathrm{Spec}\, \mathcal{F}_w$. To ease notations, let

$$\mathcal{G}(X_n) := \mathrm{Im}\left\{ H^1_{fl}(X_n, E[p^\infty]) \to \prod_{v_n \in \mathcal{M}_{F_n}} H^1_{fl}(X_{v_n}, E[p^\infty])/\,\mathrm{Im}\,\kappa_{v_n} \right\}$$

(analogous definition for $\mathcal{G}(\mathcal{X})$).
Just like in the previous section we have a diagram

$$\begin{tikzcd}
\mathrm{Sel}_E(F_n)_p \arrow[r, hook] \arrow[d, "a_n"] & H^1_{fl}(X_n, E[p^\infty]) \arrow[r, two heads] \arrow[d, "b_n"] & \mathcal{G}(X_n) \arrow[d, "c_n"] \\
\mathrm{Sel}_E(\mathcal{F})_p^{\Gamma_n} \arrow[r, hook] & H^1_{fl}(\mathcal{X}, E[p^\infty])^{\Gamma_n} \arrow[r] & \mathcal{G}(\mathcal{X}).
\end{tikzcd}$$

5.1. The map b_n.

The map $\mathcal{X} \to X_n$ is a Galois covering with Galois group Γ_n. In this context the Hochschild-Serre spectral sequence holds by [11, III.2.21 a),b) and III.1.17 d)]. Therefore one has an exact sequence

$$H^1(\Gamma_n, E[p^\infty](\mathcal{F})) \hookrightarrow H^1_{fl}(X_n, E[p^\infty]) \to H^1_{fl}(\mathcal{X}, E[p^\infty])^{\Gamma_n} \to H^2(\Gamma_n, E[p^\infty](\mathcal{F}))$$

which fits in the diagram above (note that the first and last elements are Galois cohomology groups).

Since $E[p^\infty](\mathcal{F})$ is a finite p-primary group (by Lemma 3.2) and Γ_n is a pro-l-group, one has

$$H^i(\Gamma_n, E[p^\infty](\mathcal{F})) = 0 \quad (i = 1, 2)$$

and $\mathrm{Ker}\, b_n = \mathrm{Coker}\, b_n = 0$ as well.

5.2. The map c_n.

First of all we note that $\operatorname{Ker} c_n$ embeds into the kernel of the map

$$d_n : \prod_{v_n \in \mathcal{M}_{F_n}} H^1_{fl}(X_{v_n}, E[p^\infty])/\operatorname{Im}\kappa_{v_n} \longrightarrow \prod_{w \in \mathcal{M}_{\mathcal{F}}} H^1_{fl}(\mathcal{X}_w, E[p^\infty])/\operatorname{Im}\kappa_w$$

and we only consider the maps

$$d_w : H^1_{fl}(X_{v_n}, E[p^\infty])/\operatorname{Im}\kappa_{v_n} \longrightarrow H^1_{fl}(\mathcal{X}_w, E[p^\infty])/\operatorname{Im}\kappa_w$$

separately. Observe that:

1. for any v_n there are as many maps d_w as many primes w of $\mathcal{F}$ dividing v_n but all these maps have isomorphic kernels;

2. $\operatorname{Ker} c_n \subseteq \prod_{v_n \in \mathcal{M}_{F_n}} \bigcap_{w|v_n} \operatorname{Ker} d_w$.

The Kummer exact sequence yields a diagram

$$\begin{array}{ccc} H^1_{fl}(X_{v_n}, E[p^\infty])/\operatorname{Im}\kappa_{v_n} & \hookrightarrow & H^1_{fl}(X_{v_n}, E)[p^\infty] \\ \Big\downarrow{\scriptstyle d_w} & & \Big\downarrow{\scriptstyle h_w} \\ H^1_{fl}(\mathcal{X}_w, E[p^\infty])/\operatorname{Im}\kappa_w & \hookrightarrow & H^1_{fl}(\mathcal{X}_w, E)[p^\infty]. \end{array}$$

Again $\mathcal{X}_w \to X_{v_n}$ is a Galois covering so the Hochschild-Serre spectral sequence implies

$$\operatorname{Ker} d_w \hookrightarrow \operatorname{Ker} h_w \simeq H^1(\Gamma_{v_n}, E(\mathcal{F}_w))[p^\infty] = \varinjlim_k H^1(\Gamma_{v_n}, E(\mathcal{F}_w))[p^k].$$

But $H^1(\Gamma_{v_n}, E(\mathcal{F}_w))[p^k] = 0$ because it consists of the p^k-torsion of the cohomology of a pro-l-group.

This yields $\operatorname{Ker} c_n = 0$ and therefore a_n is an isomorphism. □

5.3. Structure of $\mathrm{Sel}_E(\mathcal{F})_r$ for $r \neq l$.

The Selmer groups $\mathrm{Sel}_E(\mathcal{F})_r$ are modules over the ring $\mathbb{Z}_r[[\Gamma]]$ and, to apply the generalized Nakayama's Lemma of [1] (*i.e.*, Theorem 3.6 above), we need an ideal J of $\mathbb{Z}_r[[\Gamma]]$ such that $J^n \to 0$. The classical augmentation ideal I does not verify this condition since $I = I^2$ (see [2, Lemma 3.7]).

Anyway we can use the ideal rI to obtain a partial description of $\mathrm{Sel}_E(\mathcal{F})_r$. We need the following (detailed proof in [2, Lemma 3.8]).

Lemma 5.2. — *Let M be a discrete $\mathbb{Z}_r[[\Gamma]]$-module and $m_r : M \to M$ the multiplication by r. Then*

$$M^\vee/rIM^\vee \simeq (m_r^{-1}(M^\Gamma))^\vee = (M^\Gamma + M[r])^\vee$$

(where $M[r]$ is the r-torsion of M).

Proof. — Let $N = M^\vee$ so that N is a $\mathbb{Z}_r[[\Gamma]]$-module. Via the dual of the natural projection map $\pi : N \twoheadrightarrow N/rIN$ one sees that

$$(N/rIN)^\vee \simeq m_r^{-1}((N^\vee)^\Gamma),$$

which yields

$$M^\vee/rIM^\vee \simeq (m_r^{-1}(M^\Gamma))^\vee.$$

Since $H^1(\Gamma, M[r]) = 0$ one has $m_r(M)^\Gamma = m_r(M^\Gamma)$ and can conclude noting that

$$m_r^{-1}(M^\Gamma) = m_r^{-1}(m_r(M^\Gamma)) = M^\Gamma + M[r].$$

□

Corollary 5.3. — *Assume that both* $\mathrm{Sel}_E(F)_r$ *and* $\mathrm{Sel}_E(\mathcal{F})_r[r]$ *are finite. Then* $\mathrm{Sel}_E(\mathcal{F})_r^\vee$ *is a finitely generated* $\mathbb{Z}_r[[\Gamma]]$*-module.*

Proof. — By the previous lemma with $M = \mathrm{Sel}_E(\mathcal{F})_r$ one has

$$\mathrm{Sel}_E(\mathcal{F})_r^\vee/rI\,\mathrm{Sel}_E(\mathcal{F})_r^\vee \simeq (\mathrm{Sel}_E(\mathcal{F})_r^\Gamma + \mathrm{Sel}_E(\mathcal{F})_r[r])^\vee$$

so this quotient is finite by hypothesis and Theorems 4.16 or 5.1. Then Theorem 3.6 yields our corollary. □

In the corollary it would be enough to assume that $\mathrm{Sel}_E(F)_r$ and $\mathrm{Sel}_E(\mathcal{F})_r[r]$ are cofinitely generated modules over $\mathbb{Z}_r[[\Gamma]]/rI\mathbb{Z}_r[[\Gamma]]$. Unfortunately even with the stronger assumption of finiteness we can't go further (*i.e.*, we are not able to see whether $\mathrm{Sel}_E(\mathcal{F})_r^\vee$ is a torsion $\mathbb{Z}_r[[\Gamma]]$-module or not) due to our lack of understanding of the structure of $\mathbb{Z}_r[[\Gamma]]$-modules even for simpler Γ's like for example $\Gamma \simeq \mathbb{Z}_l$.

Appendix A. $\mathbb{Z}_l$-extensions of a field

Let F be a field, on which we assume only that $\boldsymbol{\mu}_{l^\infty} \subset F$, with $l \neq \mathrm{char}(F)$ a prime. Everything is taking place in a fixed separable closure F^{sep}. The goal is to describe the set of all $\mathbb{Z}_l^d$-extensions of F in F^{sep}.

Define $\widehat{F^*}$ as the l-adic completion of F^*: that is, $\widehat{F^*} := \varprojlim F^*/(F^*)^{l^n}$. This is a topological $\mathbb{Z}_l$-module (each quotient $F^*/(F^*)^{l^n}$ is given the discrete topology) and the natural map $F^* \to \widehat{F^*}$ has dense image.

Let $V := \mathbb{Q}_l \otimes_{\mathbb{Z}_l} \widehat{F^*}$. Then V is a topological $\mathbb{Q}_l$-vector space, complete and locally convex, with a distinguished lattice $\widehat{F^*}$ (more precisely, V is a Banach space over $\mathbb{Q}_l$, with the norm induced by taking $\widehat{F^*}$ as unit ball). The natural map $\widehat{F^*} \to V$ is an injection.

The reader is reminded that, if W is a vector space, the Grassmannian $\mathrm{Grass}_d(W) \subset \mathbb{P}(\Lambda^d W)$ is the set of all d-dimensional subspaces of W.

Theorem A.1. — *The set of $\mathbb{Z}_l^d$-extensions of F is in bijection with* $\mathrm{Grass}_d(V)$.

Proof. — By the assumption on $\boldsymbol{\mu}_{l^\infty}$, we have that $\mathbb{Z}_l(1) := \varprojlim \boldsymbol{\mu}_{l^n}$ is isomorphic to $\mathbb{Z}_l$ as G_F-module. Hence a $\mathbb{Z}_l^d$-extension $\mathcal{F}/F$ is uniquely determined by the kernel of a continuous homomorphism $G_F \to \mathbb{Z}_l(1)^d$ with image a rank d submodule ($\mathbb{Z}_l(1)$ is given the profinite topology).

We have

$$\begin{aligned}\mathrm{Hom}_{\mathrm{cont}}(G_F, \mathbb{Z}_l(1)^d) &\simeq \mathrm{Hom}_{\mathrm{cont}}(G_F, \mathbb{Z}_l(1))^d \\ &\simeq \big(\varprojlim \mathrm{Hom}(G_F, \boldsymbol{\mu}_{l^n})\big)^d \simeq \widehat{F^*}^d\end{aligned}$$

where all isomorphisms[(2)] are almost tautological but the last one, which comes from Hilbert 90 and the observation that the diagram

$$\begin{array}{ccc} F^*/(F^*)^{l^{n+1}} & \longrightarrow & \mathrm{Hom}(G_F, \boldsymbol{\mu}_{l^{n+1}}) \\ \downarrow & & \downarrow \\ F^*/(F^*)^{l^n} & \longrightarrow & \mathrm{Hom}(G_F, \boldsymbol{\mu}_{l^n}) \end{array}$$

commutes. Here, for any n, horizontal maps are the Kummer homomorphisms sending $a \in F^*/(F^*)^{l^n}$ to $\sigma \mapsto \frac{\sigma \sqrt[l^n]{a}}{\sqrt[l^n]{a}}$ and the right-hand vertical map is induced by raising-to-l: $\boldsymbol{\mu}_{l^{n+1}} \to \boldsymbol{\mu}_{l^n}$.

That is, any continuous homomorphism $G_F \to \mathbb{Z}_l(1)^d$ is of the form $\langle \cdot, x\rangle = \lim \langle \cdot, x_n\rangle_n$ for some $x = (x_{i,n}) \in \widehat{F^*}^d$, where

$$\langle \cdot, \cdot \rangle_n \colon G_F \times (F^*/(F^*)^{l^n})^d \to \boldsymbol{\mu}_{l^n}^d$$

is the l^nth level Kummer pairing, $\langle \sigma, y\rangle_n := (\frac{\sigma \sqrt[l^n]{y_1}}{\sqrt[l^n]{y_1}}, \dots, \frac{\sigma \sqrt[l^n]{y_d}}{\sqrt[l^n]{y_d}})$.

Let $\mathcal{F}_x \subset F^{\mathrm{sep}}$ be the fixed field of $\ker\langle \cdot, x\rangle$ and B_x the closure of the subgroup of $\widehat{F^*}$ generated by $x_1, \dots, x_d$. It is well-known that $F_{x,n} := F(\sqrt[l^n]{x_{1,n}}, \dots, \sqrt[l^n]{x_{d,n}})$ is the fixed field of $\ker\langle \cdot, x_n\rangle_n$ and that

$$\mathrm{Gal}(F_{x,n}/F) \simeq G_F / \ker\langle \cdot, x_n\rangle_n$$

(2) These are isomorphisms of topological groups, giving to $\mathrm{Hom}_{\mathrm{cont}}(G_F, \bullet)$ the compact open topology. Notice that since $\boldsymbol{\mu}_{l^n}$ is discrete so is also $\mathrm{Hom}(G_F, \boldsymbol{\mu}_{l^n})$.

is the dual of $B_x/(\widehat{F^*})^{l^n}$. It follows that $\mathcal{F}_x = \bigcup_n F_{x,n}$ (since $\ker\langle\cdot,x\rangle = \cap\ker\langle\cdot,x_n\rangle_n$) and that $\mathrm{Gal}(\mathcal{F}_x/F)$ is (non-canonically) isomorphic to $B_x \simeq \varprojlim B_x/(\widehat{F^*})^{l^n}$ (because any finite abelian group is non-canonically isomorphic to its dual).

In the same way, one sees that $\mathcal{F}_x = \mathcal{F}_y$ if and only if $B_x \otimes \mathbb{Q}_l = B_y \otimes \mathbb{Q}_l$.

The theorem follows. $\square$

Example A.2. — Let $F = \overline{\mathbb{F}}_p(T)$ and choose a family $a_i \in \overline{\mathbb{F}}_p$, $i \in \mathbb{N}$ and $a_i \neq a_j$ if $i \neq j$. Put $\pi_i := T + a_i$ and consider the sequence

$$x_1 = \pi_1,\ x_2 = x_1\pi_2^l,\ x_3 = x_2\pi_3^{l^2}\ \cdots\ x_{n+1} = x_n\pi_{n+1}^{l^n}.$$

The elements x_i provide a $\mathbb{Z}_l$-extension

$$\mathcal{F}_x = \bigcup_{n\in\mathbb{N}} F(\sqrt[l^n]{x_n})$$

ramified at all the π_i's.

BIBLIOGRAPHY

[1] P. N. Balister & S. Howson, "Note on Nakayama's lemma for compact Λ-modules", *Asian J. Math.* **1** (1997), no. 2, p. 224-229.

[2] A. Bandini & I. Longhi, "Control theorems for elliptic curves over function fields", *Int. J. Number Theory* **5** (2009), no. 2, p. 229-256.

[3] A. Bandini, I. Longhi & S. Vigni, "Torsion points on elliptic curves over function fields and a theorem of Igusa", to appear on Expo. Math.

[4] J. S. Ellenberg, "Selmer groups and Mordell-Weil groups of elliptic curves over towers of function fields", *Compos. Math.* **142** (2006), no. 5, p. 1215-1230.

[5] L. A. Fastenberg, "Mordell-Weil groups in procyclic extensions of a function field", *Duke Math. J.* **89** (1997), no. 2, p. 217-224.

[6] R. Greenberg, "Iwasawa theory for elliptic curves", in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, p. 51-144.

[7] ———, "Introduction to Iwasawa theory for elliptic curves", in *Arithmetic algebraic geometry (Park City, UT, 1999)*, IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, p. 407-464.

[8] A. Grothendieck, *Revêtements étales et groupe fondamental (SGA 1)*, Documents Mathématiques (Paris), 3, Société Mathématique de France, Paris, 2003, xviii+327 pages.

[9] J.-i. Igusa, "Fibre systems of Jacobian varieties. III. Fibre systems of elliptic curves", *Amer. J. Math.* **81** (1959), p. 453-476.

[10] B. Mazur, "Rational points of abelian varieties with values in towers of number fields", *Invent. Math.* **18** (1972), p. 183-266.

[11] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980, xiii+323 pages.

[12] ———, "Jacobian varieties", in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, New York, 1986, p. 167-212.

[13] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder, xviii+571 pages.

[14] J. Neukirch, A. Schmidt & K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2000, xvi+699 pages.

[15] T. Ochiai & F. Trihan, "On the Selmer groups of abelian varieties over function fields of characteristic $p > 0$", *Math. Proc. Cambridge Philos. Soc.* **146** (2009), no. 1, p. 23-43.

[16] A. Pál, "Proof of an exceptional zero conjecture for elliptic curves over function fields", *Math. Z.* **254** (2006), no. 3, p. 461-483.

[17] J.-P. Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg, viii+241 pages.

[18] T. Shioda, "An explicit algorithm for computing the Picard number of certain algebraic surfaces", *Amer. J. Math.* **108** (1986), no. 2, p. 415-432.

[19] ———, "On the Mordell-Weil lattices", *Comment. Math. Univ. St. Paul.* **39** (1990), no. 2, p. 211-240.

[20] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986, xii+400 pages.

[21] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994, xiv+525 pages.

[22] ———, "The rank of elliptic surfaces in unramified abelian towers", *J. Reine Angew. Math.* **577** (2004), p. 153-169.

[23] F. Trihan, "On the Iwasawa Main Conjecture of abelian varieties over function fields of characteristic $p > 0$", in progress.

[24] D. Ulmer, "Elliptic curves with large rank over function fields", *Ann. of Math. (2)* **155** (2002), no. 1, p. 295-315.

[25] ———, "Jacobi sums, Fermat Jacobians, and ranks of abelian varieties over towers of function fields", *Math. Res. Lett.* **14** (2007), no. 3, p. 453-467.

Manuscrit reçu le 15 juillet 2008,
révisé le 17 octobre 2008,
accepté le 16 janvier 2009.

Andrea BANDINI
Università della Calabria
Dipartimento di Matematica
via P. Bucci - Cubo 30B
87036 Arcavacata di Rende (CS) (Italy)
bandini@mat.unical.it

Ignazio LONGHI
National Taiwan University
Department of Mathematics
N° 1 section 4 Roosevelt Road
Taipei 106 (Taiwan)
longhi@math.ntu.edu.tw